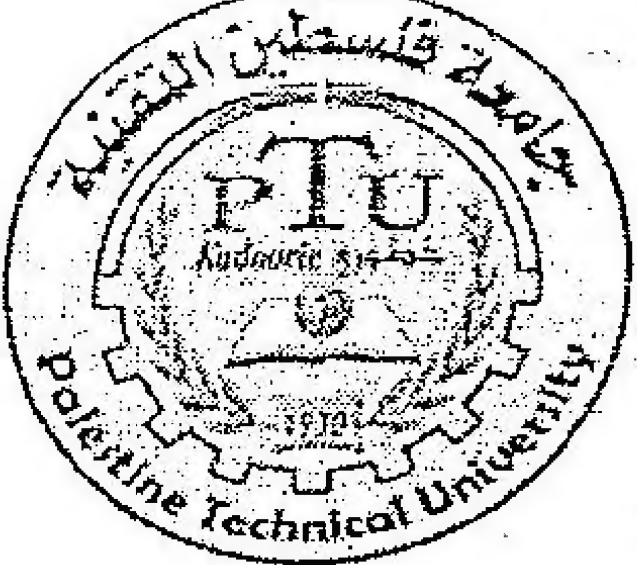


Answer Key

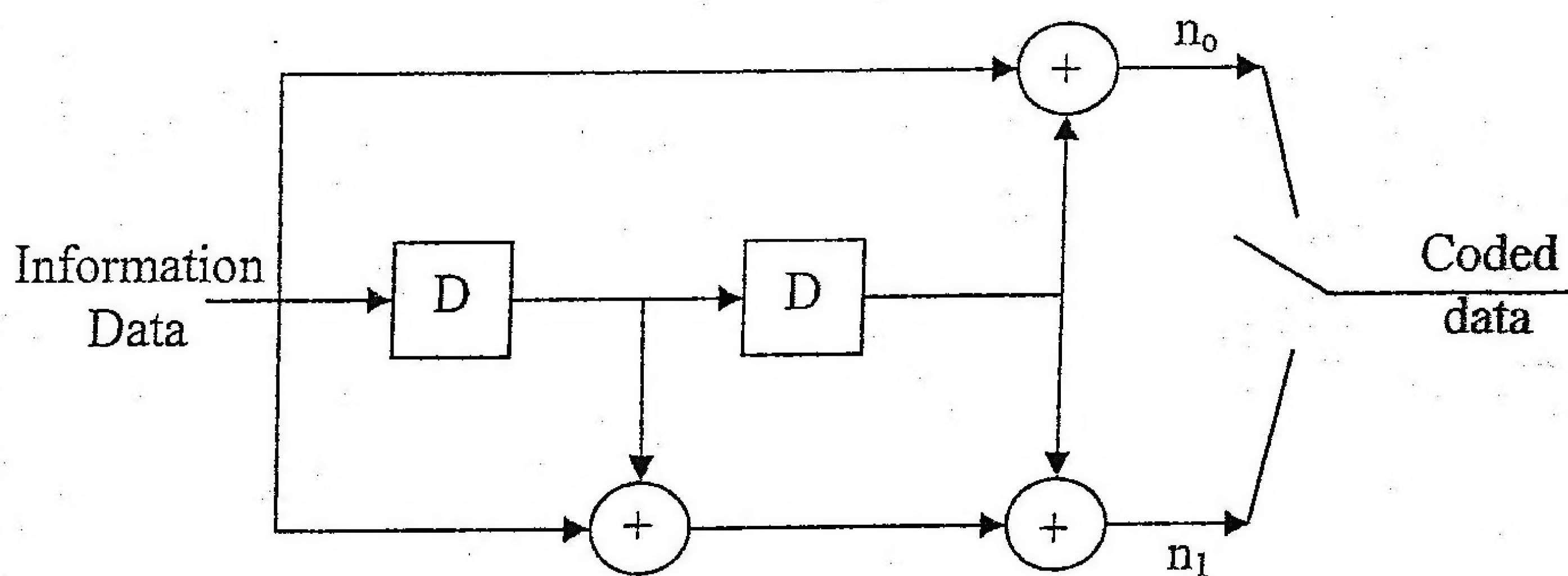
نظريه المعلومات - نهائي

Specialization:	Electrical Engineering		Palestinian National Authority Ministry Education & Higher Education Palestine Technical University College of Engineering & Technology
Course Name:	Information Theory and Coding		
Date:	28/05/2011		
Time:	8:30-10:30		
Instructor:	Dr. Mutamed Khatib		Final Exam Second semester 2010/2011

Answer *all* the following 5 questions

Q1. (8 marks) Find the entropy, redundancy and information rate for a four-symbol source (A, B, C, D) with a baud rate of 1024 symbols/s and symbol selection probabilities of 0.2, 0.5, 0.2, 0.1 under the condition that the source has one-symbol memory location such that no two consecutively selected symbols can be the same.

Q2. (8 marks) Encode the sequence 1000 ($I_0 I_1 I_2 I_3$) using the rate $\frac{1}{2}$ constraint length 3 binary (2,1,3) convolutional code, with the encoder below:



Q3. (8 marks) Use Public Key Encryption method to encrypt the plane-text message number 21. Choose the smallest possible values of P and Q . Decipher the resulting cipher-text to check your answer

Q4. (8 marks) Consider the random variable

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0.5	0.26	0.11	0.04	0.04	0.03	0.02

- Find a binary Huffman code for X .
- Find the expected code length for this encoding.

Q5 (8 marks) Given a $\frac{1}{2}$ rate convolutional encoder defined by $P_1(x) = 1 + x + x^2$ and $P_2(x) = 1 + x^2$, and assuming data is fed into the shift register 1 bit at a time, draw the encoder tree diagram.

Good luck

تم الرفع بواسطه
م. محمد ابو عيسى

Q.1

$$P(A|A) = P(B|B) = P(C|C) = P(D|D) = 0$$

$$P(B) = 0.5 \Rightarrow P(\bar{B}|B) = P(B|\bar{B}) = 1 \quad \bar{B}: \text{not } B$$

$$\Rightarrow P(A|B) + P(C|B) + P(D|B) = 1$$

$$P(B|A) + P(B|C) + P(B|D) = 1$$

$$P(A|C) = P(A|D) = P(C|A) = P(C|D) = P(D|A) = P(D|C) = 0$$

$$P(A) = P(A|A)P(A) + P(A|B)P(B) + P(A|C)P(C) + P(A|D)P(D)$$
$$0.2 = 0 + P(A|B)0.5 + 0 + 0$$

$$\Rightarrow P(A|B) = \frac{0.2}{0.5} = 0.4$$

$$P(C) = P(C|A)P(A) + P(C|B)P(B) + P(C|C)P(C) + P(C|D)P(D)$$
$$0.2 = 0 + P(C|B)0.5 + 0 + 0$$

$$\Rightarrow P(C|B) = \frac{0.2}{0.5} = 0.4$$

$$P(D) = P(D|A)P(A) + P(D|B)P(B) + P(D|C)P(C) + P(D|D)P(D)$$
$$0.1 = 0 + P(D|B)0.5 + 0 + 0$$

$$\Rightarrow P(D|B) = \frac{0.1}{0.5} = 0.2$$

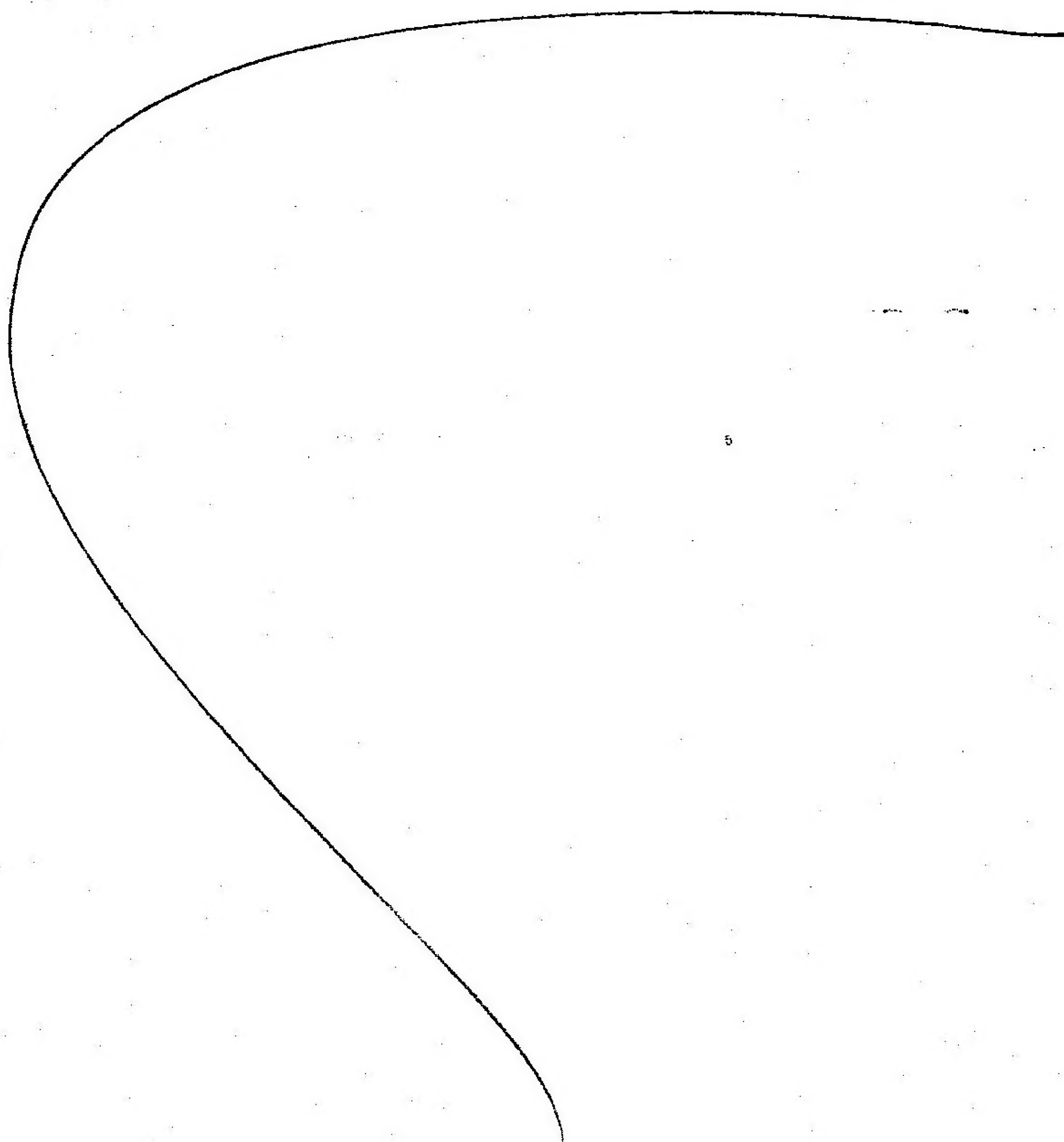
$$H = \sum_i P(i) \sum_j P(j|i) \log_2 \frac{1}{P(j|i)} \quad \text{bit/symbol.}$$

$$= P(A) \left[P(A|A) \log_2 \frac{1}{P(A|A)} + P(B|A) \log_2 \frac{1}{P(B|A)} + P(C|A) \log_2 \frac{1}{P(C|A)} + P(D|A) \log_2 \frac{1}{P(D|A)} \right]$$
$$+ P(B) \left[P(A|B) \log_2 \frac{1}{P(A|B)} + P(B|B) \log_2 \frac{1}{P(B|B)} + P(C|B) \log_2 \frac{1}{P(C|B)} + P(D|B) \log_2 \frac{1}{P(D|B)} \right]$$
$$+ P(C) \left[P(A|C) \log_2 \frac{1}{P(A|C)} + P(B|C) \log_2 \frac{1}{P(B|C)} + P(C|C) \log_2 \frac{1}{P(C|C)} + P(D|C) \log_2 \frac{1}{P(D|C)} \right]$$
$$+ P(D) \left[P(A|D) \log_2 \frac{1}{P(A|D)} + P(B|D) \log_2 \frac{1}{P(B|D)} + P(C|D) \log_2 \frac{1}{P(C|D)} + P(D|D) \log_2 \frac{1}{P(D|D)} \right]$$

$$\Rightarrow H = 0.2 \left[0 + 4 \log_2 \frac{1}{4} + 0 + 0 \right] + 0.5 \left[0.4 \log_2 \frac{1}{0.4} + 0 + 0.4 \log_2 \frac{1}{0.4} + 0.2 \log_2 \frac{1}{0.2} \right] \\ + 0.2 \left[0 + 1 \log_2 1 + 0 + 0 \right] + 0.1 \left[1 \log_2 1 + 1 \log_2 1 + 0 + 0 \right] \\ = 0.761 \text{ bit/symbol.}$$

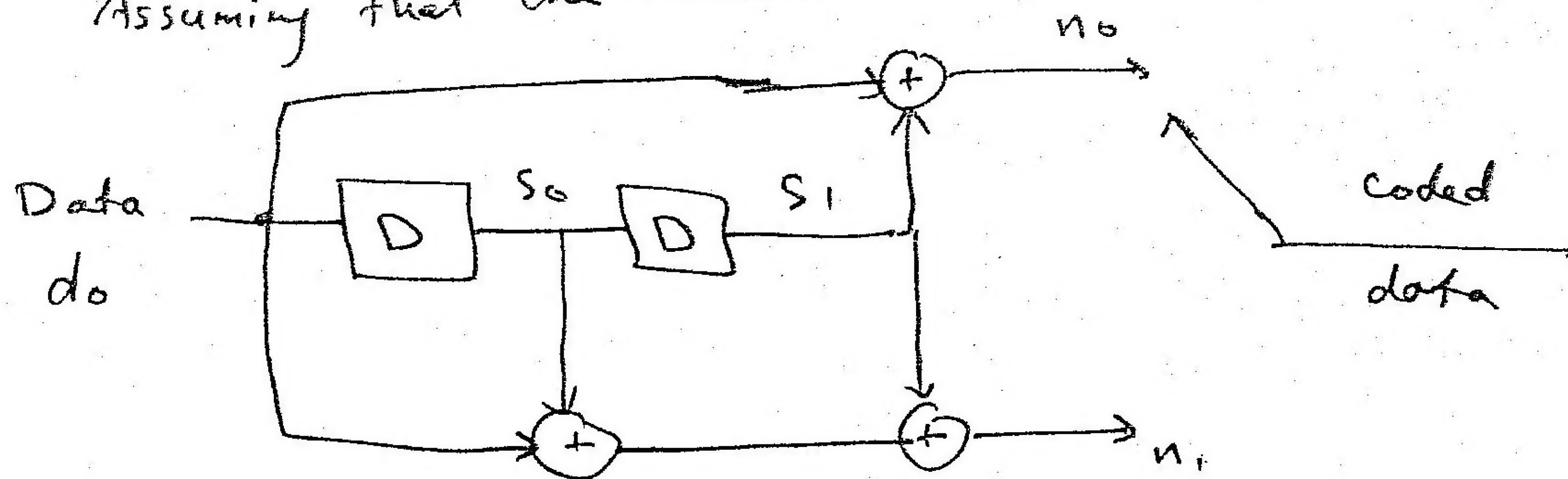
$$R = H_{\max} - H = \log_2 4 - 0.761 = 1.239 \text{ bit/symbol.}$$

$$R_i = R_s H = 1024 \times 0.761 = 779 \text{ bit/s.}$$



Q.2 There is only one data bit per block, and hence no need for an input demultiplexer, and two code bits, generated by the 2 sets of modulo 2 adders shown.

Assuming that the encoder starts from zero state:



d_0	S_0	S_1	n_0	n_1
1	0	0	1	1
0	1	0	0	1
0	0	1	1	1
0	0	0	0	0

\Rightarrow coded data 1101100

Q.3 $T = 2$

$$C = T^N \bmod N$$

$$N > T$$

$$N = PQ \Rightarrow P = 5 ; Q = 7 \Rightarrow N = 5 \times 7 = 35$$

$$C = 2^{35} \bmod 35 = 18$$

STR to decipher :

$$T = C^{P'} \bmod Q \text{ where } PP' = 1 \bmod (Q-1)$$

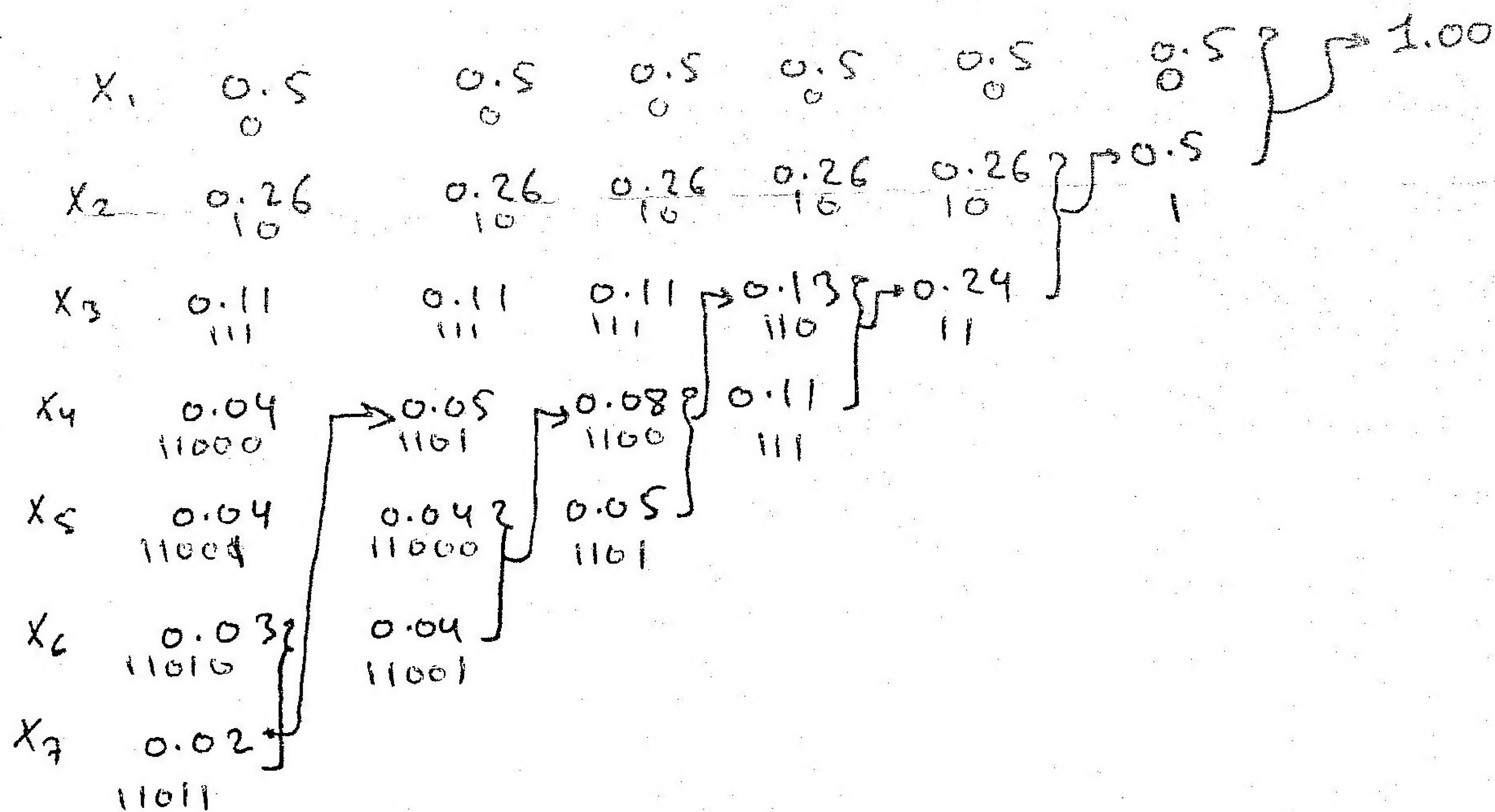
$$\Rightarrow 5P' = 1 \bmod 6 \Rightarrow 5P' = 7, 13, 19, 25, 31,$$

x x x x

$$\Rightarrow P' = 5$$

$$\Rightarrow T = 18^5 \bmod 7 = 2$$

Q.4



	X_1	X_2	X_3	X_4	X_5	X_6	X_7
code	0	10	111	11000	11001	11010	11011
L	1	2	3	5	5	5	5
P	0.5	0.26	0.11	0.04	0.04	0.03	0.02

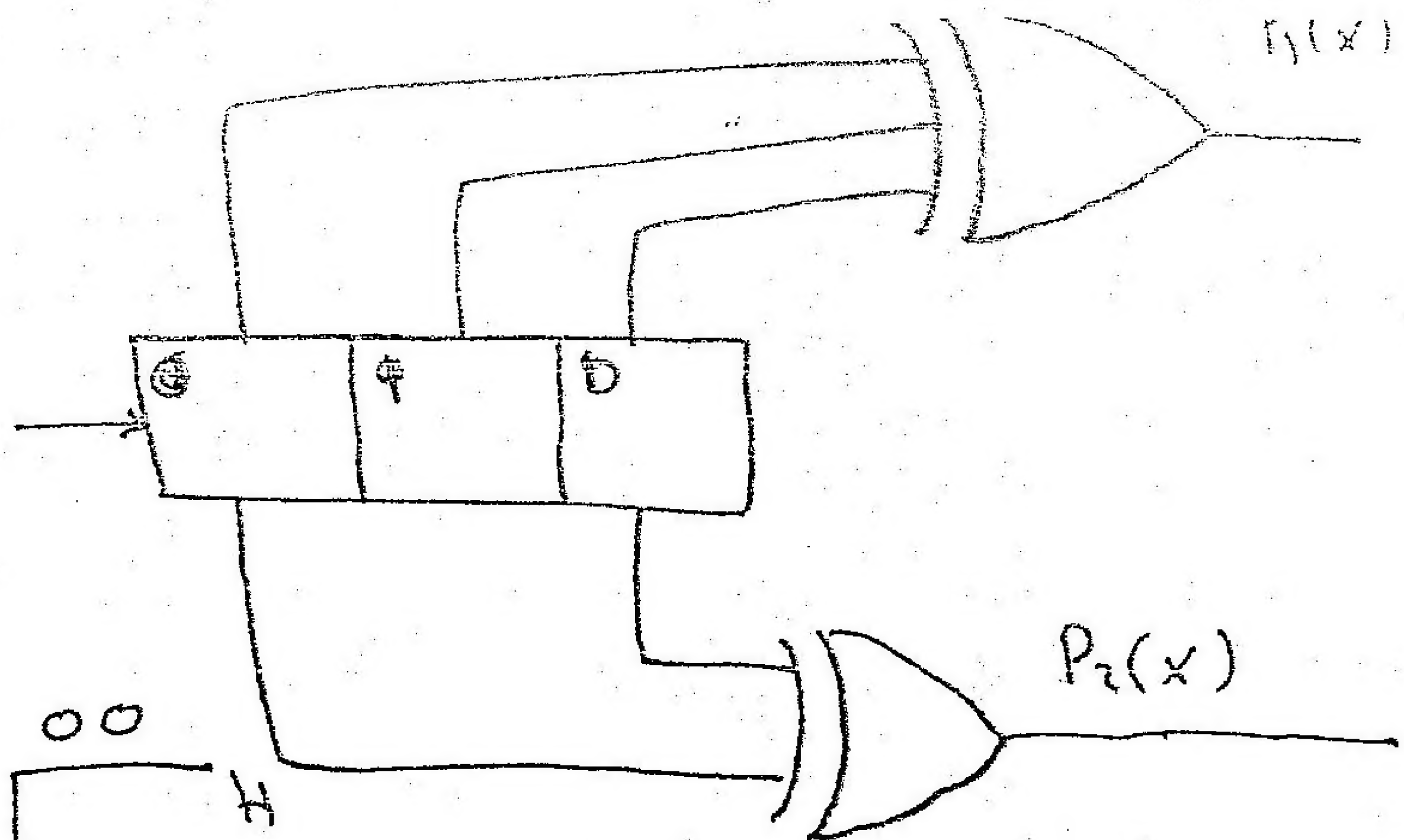
$$H = 0.5 \times 1 + 0.26 \times 2 + 0.11 \times 3 + 0.04 \times 5 + 0.04 \times 5 + 0.03 \times 5 + 0.02 \times 5$$

$$= 2$$

\Rightarrow Expected length is 2

Q.5 $P_1(x) = 1 + x + x^2$

$P_2(x) = 1 + x^2$



Tree diagram

